SEQUOIA
voting systems

Election Reform Update

Presented to Election Assistance Commission by Sequoia Voting Systems
May 5, 2004

Sequoia Voting Systems has been providing election equipment, supplies and services for more than 100 years. In our history, we have provided election officials with lever machines, punch card voting systems, optical scan voting equipment and for the last 25 years, we have helped election officials conduct extremely successful elections with two different types of direct recording electronic voting systems.

There are currently more than 50,000 Sequoia DRE units installed across the country which will be used to securely and accurately record more than 105 million individual votes for candidates and issues this November.

The voters that use these systems can be confident that the votes they record will be cast on the most accurate, reliable, user-friendly, accessible and secure voting technology that has been deployed in this country's history.

With more than 500 pages of federal voting systems standards, reviews by two federally approved independent testing authorities, additional state testing, the escrow of software source code, the pre-election testing of each DRE machine and the increased levels of security that DRE systems provide over and above paper-based systems, voters can take great confidence that the November 2004 election will be the most complete and accurate recording of voter intent this country has ever seen.

Mechanical voting methods have been used to record votes for more than 100 years. Computers have been used for the last 35 years. Direct recording electronic voting systems have been available for 25 years and have been widely used for the last 15 years.

As we learned in 2000, the complexity of older voter interfaces have unfortunately caused a large number of voters to make errors and have placed election officials in the precarious position of discerning voter intent on ambiguously marked ballots. Not only were older systems more susceptible to error and abuse, but they also prevented a large number of voters from casting ballots that were physically accessible to people with disabilities. Voting in a language other than English was often cumbersome or impossible.

There is little doubt that the current generation of DRE systems provides considerable improvements to the voting process, however, what has been left out of the recent public debate is that not only has DRE voting technology been used reliably for more than two decades, but the systems also provide considerable improvements to ballot security and auditability.

For example, the Sequoia touch screen voting system provides five different methods of conducting a recount of ballots and, when configured with our VeriVote printer, can provide two additional methods of reconstructing an election.

By contrast, a punch card system or a central count optical scan voting system has only two methods of permitting a recount. If paper ballots are lost, damaged or destroyed – there is no way to reconstruct those records or conduct a recount at all. That is not the case with electronic machines that immediately create redundant records of all votes cast.

Successful election administration relies on several inter-related pieces that that involve technology, people and procedures. To gain an accurate picture of the state of election administration and voting in this country, it is important to look at these issues individually, but more important to look at them as a collective whole.

Much of the recent public debate about electronic voting systems has focused on individual aspects of voting technology – specifically the security and reliability of the software code that resides in the systems. However, individual technological components are only one piece of the election puzzle. Of equal or greater importance to the election improvements contemplated by the Help America Vote Act will be the people and the procedures that help us maximize the benefits and minimize the risks of election modernization.

Attached to this document, we have included a high-level security summary of the technological and procedural safeguards utilized in our AVC Edge and AVC Advantage electronic voting systems.

To help understand the technological and the procedural safeguards in place, it is important to understand the lifecycle of a DRE election and compare it to a similar review of paper-based elections.

The following steps help explain the manner in which one California county implements their touch screen voting system:

Federal Qualification and State Certification

Before a system is purchased, virtually all jurisdictions in the country require the system to meet or exceed federal voting systems standards.

The 2002 voting systems standards contain approximately 500 pages of detailed security and performance requirements that must be met before a system is deemed federally qualified.

For a system to achieve federal qualification status, the hardware must be extensively tested and approved by federally sanctioned hardware testing laboratory. The firmware code used in the voting system is subjected to a line-by-line review by the laboratory and the system must pass a number of extensive performance and environmental tests.

The software is submitted to a separate laboratory which must also be federally-sanctioned to conduct a line-by-line code review and a series of detailed performance tests to ensure compliance with the federal voting systems standards.

Once the two testing laboratories approve the hardware and software, the system is then reviewed by a technical advisory board of the National Association of State Election Directors.

At the state level, additional tests and a review of source code and functional requirements specific to the state are often conducted as a condition of state certification.

When a system is upgraded or changed, it must be re-submitted for another round of federal testing. Federal testing can take anywhere from two to six months or more depending on the components tested.

Acceptance Testing

Once a system is federally qualified, state certified, purchased by a local jurisdiction, and delivered to election officials, considerable local testing is done to ensure the system delivered meets the proper specifications.

Logic and Accuracy Testing

To guarantee that the voting system counts votes exactly as they are cast by voters, the local officials will conduct a "logic and accuracy test" on every voting machine before each election. These tests include the casting of a specific known quantity of votes and comparing the number of votes recorded to the number of votes entered into the machine. These tests require and demonstrate 100% accuracy of the vote counting process.

After the election, the same tests are often conducted to demonstrate that the vote counting software has not been altered in any way.

Escrow of Source Code

To protect against any possibility that malicious software code is included in the voting system, an exact copy of the software used to conduct the election is stored in escrow with many Secretaries of State.

System Design and Election Procedures

In a moderate to large county, the Sequoia AVC Edge voting system may include five voting machines per precinct and in approximately one thousand polling places. Each machine is a stand-alone device. It is never connected to the Internet or to any other network that would provide the public with access to the Edge's operating system or software.

To prevent any attempt to access the software, each of the machines is delivered to polling places with a uniquely numbered tamper-evident seal that secures the vote cartridge from public access until after the polls are closed.

A similar seal is also used to protect the switch that allows polls to be opened and closed.

For someone to alter the code of a voting machine, they would have to break the numbered seal, reverse-engineer the proprietary voting software, create new software that would produce their desired result for each of the hundreds of different ballot styles in the county and insert it back into each of the 5,000 voting machines in front of approximately 4,000 poll workers. They would also need to make sure that the eventual number of votes recorded matched the number of signatures collected on each precinct's poll roster throughout the county.

Once this feat was accomplished, the hacker(s) would then have to make sure they were able to replicate the identical seals with the identical serial numbers for each machine -- again without detection by a single poll worker.

Redundant Memory

Throughout the voting process, each ballot is recorded in multiple locations within the Edge. The memory inside the machine also performs an automated review to ensure that the accumulated data on each form of memory is identical after each vote is recorded.

The results cartridge is removed by poll workers at the close of the polls and is sent to the county for tabulation. That cartridge is capable of producing both the summary of the votes as well as a copy of each individual ballot. If for any reason, the results cartridge is lost or destroyed, a new cartridge can be created from the alternative memory source that remains in the Edge.

Sequoia's Proprietary Operating System

While Election Day procedures and logistics make it impossible to access the source code on voting machines, Sequoia has taken the additional precaution of utilizing a proprietary operating system inside our touch screen voting machines.

Off-the-shelf operating systems dominate the marketplace and are often the preferred vehicle for the vast majority of all viruses, Trojan Horses, and other malicious code. By using a proprietary operating system, Sequoia offers an extra layer of security that other systems do not.

Paper Audit Trail of Individual Ballots

The Edge has the ability to print vote totals from each machine as well as a replica of every ballot cast on each machine or in each precinct. These ballot images are stored randomly within the touch screen unit to ensure the secrecy of each voter's ballot.

Complete ballot images can be printed at the polling place when the polls close or via high speed printers at the central counting facility. The printed ballots can be generated either from the touch screen units, from the vote cartridges themselves or from the central vote counting system.

Ballot Images as Verification of Central Counting System

Because the equipment used by voters is not susceptible to manipulation by outside sources, it is important to ask if the central vote tallying software can be altered by inside sources.

As mentioned earlier, the vote counting software is stored in escrow prior to the election so it may be accessed in the event of any charges of malfeasance or manipulation of vote totals.

As an additional check on the system to ensure accuracy, the individual touch screen units and the removable memory cartridges both serve as accurate original source data in case ballots need to be recounted electronically or if paper ballots need to be created for a manual hand count of the vote.

These images are also used to comply with the State of California's requirement to conduct a 1% manual recount of votes cast after every election to further validate the accuracy of the vote counting software.

Importance of Perception

At Sequoia, we are certain that our voting systems meet the highest security standards in both technology design and in Election Day procedures. The comprehensive review conducted by the federal and state government in coordination with independent testing experts should provide voters with the confidence they need and deserve.

However, perception is critical in the conduct of elections. We encourage the Election Assistance Commission to be aggressive in supporting the conclusion reached by federal and state authorities. The Sequoia AVC Edge voting system is secure, it is more accurate than other voting technologies and it provides unprecedented benefits to disabled voters and voters who require assistance in alternative languages.

However, if states of local officials decide they would ultimately prefer an additional feature that will produce a voter verifiable printout of the ballot cast, Sequoia is currently in the process of requesting federal qualification of our VeriVote printer as an upgrade to the Edge touch screens. That upgrade is an additional device that can plug-into the system and print the ballot for each voter to review.

In addition to the procedural steps above, a number of additional hardware, software and physical security protections are in place in every jurisdiction served by Sequoia.

As the commissioners know, there is a community of activists, election officials and interested observers watching this ongoing public debate very closely.

While it appears at times that some of the calls for increased security, accessibility and ease of use are mutually exclusive, that is not the case.

Sequoia has developed two extremely secure, accessible and user-friendly electronic voting systems that have been deployed with great success for countless elections in the last two decades.

As new auditing features such as the contemporaneous paper record are requested or required, we will be able to meet that demand with an upgrade that is as easy for poll workers and election officials as possible while ensuring the greatest degree of accessibility for voters who need it.

In short, we at Sequoia believe that voter verifiable paper records are not a mandatory component of secure and accurate elections, however we understand the fears many people have about technology. In the very near future, Sequoia Voting Systems will offer upgrade features to new and existing DRE systems that provide the voter verifiable audit features that will address concerns of skeptics while also retaining the ease of use and accuracy of the original system design.

Throughout the history of election administration and reform, change has always caused concern, and concern and experience have always led to continuous improvements. The issues facing this panel are no different.

As the Election Assistance Commission considers the state of election reform nationally and looks at the best ways to improve the conduct of elections, please remember that for any improvement to work well, it must be easy for voters and election officials and should be implemented incrementally first. We must give human factor issues the priority they deserve.

In the end, when millions of voters and more than one million precinct officials take to the polls, it is the human interaction with the technology that will make our elections succeed or fail.

Attachments:

Sequoia AVC Edge Security Overview
Sequoia AVC Advantage Security Overview
Methods of Recounting Electronic Ballots
Sample Ballot Image Printout
Undervote Warning Messages
Sequoia Press Release Announcing Voter Verifiable Paper Records
Security Analysis Conducted by State of Nevada Gaming Control Board

Sequoia AVC Edge Security Overview

Sequoia Voting Systems, Inc.
7677 Oakport Street, Oakland, CA 94621, 510-875-1200

AVC Edge®

Security Overview

Release 4.2

INTRODUCTION

Security is a blanket term which involves a variety of elements designed to mitigate potential risks and threats. In general, secure systems will control, through use of specific features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.

The design of a secure environment involves the use of three types of *controls*:

Preventative Controls:

The purpose of this type of control is to prevent the occurrence of one or more specific risks or threats. These controls can be use as a means of restricting or limiting access to data, functionality, or components. They may also be used to directly interdict potential threats or outside attack.

Detective Controls:

All risks, threats, or attacks cannot be prevented — e.g., a system which permits outside dial-up access can use preventative control to stop unauthorized access, but it cannot prevent recurring attempts. In these cases, it is important to at least detect or record that such an event occurred. Detective controls are intended to identify real, potential, or attempted breaches in security. They are also often used to record an audit trail of activity which can be subsequently examined to identify potential problems or risks.

Corrective Controls:

Even with preventative and detective controls in place, it is possible that damage or loss could occur (e.g., an authorized person uses such authorization to damage the system). Corrective controls are procedures or mechanisms which enable recovery from the loss or damage.

The security of any system, organization, or environment is not the result of merely one or two system components. It is the result of a variety of features, controls, architectural decisions, and procedures combining and building upon each other to produce a *security infrastructure*.

Security is fundamental to the election process. Security implies that the system must be reliable, it must accurately record votes and it must maintain the integrity of those votes. Security is achieved through features and controls which are inherent in the system design and through administrative controls. The acceptable level of security cannot be achieved with just one. Both types of controls must be present. This document is an overview of the security features and controls in the design of the AVC Edge® Direct-Record Electronic voting machines.

SYSTEM OVERVIEW

The AVC Edge® Voting System consists of two major components, the AVC Edge® Electronic Voting Machine and the Election Database System (WinEDS) Central System.

The AVC Edge® incorporates a color LCD with an integral touchscreen, a control panel for use by election poll workers, appropriate electronic circuitry and processing devices for performing specified system functions, internal memory for storing ballot data and voting records, a removable Results Cartridge with non-volatile memory, protective and public counters, and integrated voter privacy panels.

The Results Cartridge is designed so that it can be inserted into the voting machine, record voting results, be removed from the machine at the closing of the polls and be read by the WinEDS Central System. The Results Cartridge stores:

- an electronic representation of the ballot,
- ballot logic to enable the voter to make those selections to which he or she is lawfully entitled,
- the aggregated vote totals,
- a randomized record of all individual ballots cast, and
- a chronological log of significant machine operations, including error conditions.

The WinEDS Central System ("WinEDS") is a computer software system which contains application software developed specifically for election requirements. The WinEDS System consists of the following subsystems:

- Election setup, which provides functions to initialize an election, define the political parties, offices and party positions, political subdivisions, types of elections and other global election variables.
- Candidate management, which allows the election office to identify the contests and candidates for an election.
- Ballot management, which provides for the layout of the visual ballots and the generation of the ballots in electronic or paper form.
- AVC Edge® management, which provides functions that helps manage AVC Edge® testing, maintenance and election preparation.
- Election results management, which provides the functions for election night tally of Results Cartridges and paper ballots (Absentee Ballots), the re-canvass of the election and the certification of all contests to the political parties and state election reporting agencies.

AVC Edge® DESIGN OVERVIEW

The AVC Edge® is a direct descendant of the very successful AVC Advantage voting machine. The AVC Advantage is a tried & true product, with a 15 year history. Over 25,000 systems are in use. In countless elections, and with countless numbers of votes cast, *not a single vote has been lost to equipment malfunction or software error.*

Security & integrity of the voting process were cornerstones of the design philosophy of the AVC Edge. The design has features that enhance system security and maximize resistance to virus and Trojan horse type attacks. These will be discussed in more detail below.

AVC Edge® SECURITY

It is helpful to look at *where* in an election cycle attacks could be mounted, so that there is a context for the security features in the system. Where can attacks be made?

- During development of the AVC Edge's software.
- During ballot definition and cartridge generation at WinEDS.
- During transport of programmed Results Cartridges to the AVC Edge® warehouse.
- During the AVC Edge® technician's Ballot Verify and Pre-LAT process.
- During the Election.
- During transport of the Results Cartridges to the tally site.
- During tabulation at WinEDS.

In a similar vein, the results of attacks on the election cycle can be categorized as:

- Denial of Service
- Alteration of Vote Data

Denial of Service attacks, which can always be of a vandalism nature, are an equal threat to all voting systems, electronic or paper based. Alteration of Vote Data attacks (or the loss of vote data) are of more importance; the sections that follow will describe the safeguards in the AVC Edge® that make such attacks closer to impossible on the AVC Edge® than with any other voting system.

One important point to also keep in mind is that a *meaningful* attack, in either category, must involve affecting a large number of votes. After programmed Results Cartridges leave WinEDS, they move into the hands of *several* AVC Edge® technicians for machine preparation, and on election day, the AVC Edges are in the hands of *hundreds* of poll workers, at multiple physical locations. Collusion at this level is unlikely to go undetected.

Loading the Ballot Onto the AVC Edge

Each AVC Edge® goes through an automatic validation process to load the WinEDS-defined ballot. It must then also go through a Pre-Election Logic & Accuracy Test (Pre-LAT). It is not possible to bypass these steps.

The ballot load and Pre-LAT operations are typically performed by AVC Edge® technicians, with the machines still in the storage warehouse.

When WinEDS generates a ballot and loads it onto a Results Cartridge, it includes the following integrity checks:

- Each Results Cartridge is "branded" with the destination AVC Edge's serial number.
- A CRC is calculated for each of the data files that comprise the ballot definition. These CRC values are stored along with the ballot data.

During the loading of a ballot, the AVC Edge® initializes itself for the upcoming election based on the ballot files read from the Results Cartridge. The ballot definition on the Results Cartridge is subjected to the following tests before it is loaded into the AVC Edge:

- The serial number on the Results Cartridge must match this AVC Edge.
- The ballot file CRC values calculated & stored by WinEDS are validated.
- Make sure there is no vote data already stored on the cartridge, of any type: Ballot images, write in names, candidate totals counters and selection code totals counters.
- Make sure that file sizes make sense, for example that there are an equal number of candidates in the ballot defintion as there are candidate summary totals counters.

Any failure in the above tests will cause the AVC Edge® to declare an error, and to reject the Results Cartridge.

Once the tests listed above are completed successfully, the data from the Results Cartridge is copied into the AVC Edge® Audit Trail memory. From this point forward the AVC Edge® will not operate without the correct Results Cartridge installed.

The Pre-Election Logic and Accuracy Test (Pre-LAT) verifies the logical correctness of the ballot and its match to the visual ballot. During this test all activity is the same as it would be in an official election and the same software logic is exercised, <u>with the important exception that the vote data is stored separately from the Official Election vote data</u>.

Voting during Pre-LAT can be either manual, or automatic via a vote simulation script. This vote simulation feature, <u>which is only available in Pre- and Post-LAT</u>, allows the ballot logic to be tested, with large numbers of votes (in excess of 100,000 candidate selections), and without the possibility of data entry errors.

Upon closing of Pre-LAT polls, the AVC Edge® generates a Pre-LAT results report. The totals can be compared to the predicted totals from manual voting or Vote Simulation scripts.

Conducting the Election

During the Election, the Results Cartridge must always be inserted in the AVC Edge®. If it is removed, the AVC Edge® will stop its normal operations, generate an error indication and make an entry in the Event Log. In addition, the Auxiliary Port must be kept empty. Attempting to insert *any* cartridge type into this port will also stop normal operations, generate an error condition and make an Event Log entry.

A numbered seal can be installed to physically ensure that the Results Cartridge is not removed.

At the opening of the polls, a zero proof report is generated which includes the poll site, precinct number, public counter and protective counter, and all ballot information with the state of the internal vote counters. This report proves to the poll site officials that the AVC Edge® has no previously stored vote data.

The process for recording votes includes the use of redundant memories, one resident on the AVC Edge CPU board (Audit Trail memory), and the other in the Results Cartridge. These memories are verified to be identical after each voter is finished, and also each time the AVC Edge® is turned on while in Election Mode. Any error or mismatch in the verification process will generate an orderly shutdown and an error message.

The vote recording process begins when the voter presses CAST VOTE. The Election Program composes the voter's Ballot Image record and increments the totals counter of each candidate that the voter selected. A CRC value is calculated and appended to each Ballot Image. This data is saved to both the Audit Trail memory on the CPU board and the Results Cartridge. All operations are double-checked (reading back data just written, etc.) during the vote saving process. After all the voter data is stored the public and protective counters are incremented. Any error that may occur during the vote save process is uniquely reported and causes the voting process to stop on this AVC Edge.

The AVC Edge® then performs an internal cross-check of the redundant memory areas (Audit Trail and Results Cartridge). This cross-check makes sure the two memories are identical, down to the bit level; it includes the vote totals and ballot image storage areas. Any discrepancy is cause for halting the voting process on this machine. Next, an internal "recount" is performed. This recount validates each ballot image and recalculates the summary totals from the ballot image data. Any mismatch between the ballot image totals and the summary total counters will be detected. After a successful cross-check, the poll worker may activate the machine for the next voter.

Since the AVC Edge® retains a ballot image record for each voter, it is important that these ballot images not be saved in the order in which they were cast as that would provide the ability to learn how an individual cast their vote. When the AVC Edge® allocates storage space for ballot images and write-in data, it takes the following steps to assure storage of this data is sufficiently random to avoid identification of voter data with individual voters.

1) Storage space is allocated in large blocks rather than on a per-voter bases. When an allocation is required, a random number of storage blocks between 50 and 100 are allocated.
2) Access to the storage blocks is via an indirect table of block numbers. This table is shuffled randomly when the blocks are allocated, so that the sequence of storing ballot images within the storage blocks is random.

The randomizing function in the AVC Edge® uses a mathematical pseudo-random number generator that is further randomized by the value of the AVC Edge's internal real time clock at the time of the random number request. This pseudo-random number generator has been reviewed by independent computer experts and been deemed sufficiently random that it would not reasonably be reversible based on the amount of data that would serve as the basis for the reversal.

Tallying Results

When polls are closed, the AVC Edge® immediately calculates and stores cryptographic signatures of each of the totals data files (ballot images, write in names, candidate summary totals, and selection code summary totals). The cryptographic signature values are stored in both the Audit Trail and Results Cartridge memories.

Next, the AVC Edge® generates a Results Report. This report shows the value of each candidate counter (including ballot measures) and also shows voter turnout data per precinct or primary party, if applicable.

Once the report is complete, the Results Cartridge can be removed and transported to the WinEDS system for tally. Typically, this transport is done in a secure manner - the cartridges are placed in a sealed case and transported by at least two poll workers.

Once at WinEDS, the cartridges are tallied. WinEDS validates the ballot definition on the cartridge to make sure the cartridge has come from the correct election definition. Cartridges that have an incorrect ballot are rejected. WinEDS also maintains lists of cartridges that were assigned to this election, and of cartridges that have already been tallied. Each time a Results Cartridge is presented for tally, it is checked against these lists.

If a question arises about the integrity or accuracy of the election night tally, several safeguards can be relied upon:

- The cryptographic signatures of the totals information can be re-validated.
- There is still a redundant copy of the vote data, and ballot, on each AVC Edge. An AVC Edge's Results Cartridge can be returned to the AVC Edge®, and the two copies verified to still match.
- The data that WinEDS tallied from the Results Cartridge can be verified against the Results Report generated by the AVC Edge® when polls closed.
- WinEDS can print data directly from a Results Cartridge. Results Reports, Ballot Image details, and the Event Log can all be printed.
- Additional copies of the Results Report can be printed from the AVC Edge's Audit Trail memory.

To test that the AVC Edge® is still operating properly, with the correct ballot, a post-election Logic and Accuracy Test (Post-LAT) can be run. This mode is functionally the same as the Pre-LAT mode, including the availaiblity of Vote Simulation.

What would happen if a Results Cartridge were lost or damaged while in transit to WinEDS for tally?
There are three backup methods for dealing with this situation. The first is to use WinEDS to manually enter the vote data for the AVC Edge, from the printed Results Report. The second method is to use a special "Audit Trail Transfer" Cartridge. This cartridge, in conjunction with a firmware function only available at polls closed, allows for transferring an exact copy of the AVC Edge's Audit Trail memory to the cartridge. WinEDS can then do its tally from this cartridge. Finally, additional copies of the Results Report can be printed from the AVC Edge's Audit Trail memory.

OTHER POINTS AND ISSUES

Can Malicious Software Be Introduced Into the AVC Edge?

No. Here are the reasons why:

In order to verify that the correct firmware is installed in each machine, Sequoia has administrative controls in place from the time the firmware is written and compiled until the time it is locked and sealed in each AVC Edge. The points in this sequence are when:

- The firmware is written and the master program created,
- The master firmware is reproduced for installation in each AVC Edge, and
- The AVC Edge® machines are delivered to a customer.

The AVC Edge® firmware is written in a high level language and is well designed and written so that it can be easily read and understood. This has been confirmed by the FEC certification process. Sequoia conducts comprehensive testing as part of the qualification acceptance testing of the AVC Edge.

The AVC Edge® software is under strict configuration management control. This means that there are verifiable means of controlling, accounting for, and verifying any and all changes to the baseline machine firmware, which has been the subject of detailed review. The firmware is compiled twice, by different people, on different computers and the results verified to be identical.

During the assembly of the AVC Edge® there are manufacturing controls to provide assurances that the correct version of firmware is being installed in each machine. Also in manufacturing there are procedures that allow Sequoia Voting Systems to verify that the known version of software is, in fact, the version installed on the AVC Edges.

Each machine is a stand alone processor. Errors cannot be promulgated from one machine to another. The machines cannot be accessed by telecommunications. Access to the machine is limited by administrative procedures and is also limited by the physical design of the machines.

In summary, there are controls from the source code review through the manufacture and delivery of the AVC Edge® to protect the integrity of the firmware. Thereafter, the AVC Edge® design limits access to the program ROMs through physical means -- locks and seals -- and logical means -- checksums at power up and program initiation. Finally, by machine design the machine is not accessible to the outside except through the Results Cartridges.

Other AVC Edge® Security Features

1) The AVC Edge® is designed to allow the attachment of seals to its various parts to ensure that there is no unauthorized access. These seals are typically serialized, and recorded on election paperwork, and they cannot be removed without destroying them. Also, the cartridges cannot be taken apart without causing physical damage, providing additional evidence of tampering.

2) The AVC Edge® uses a software-controlled power down. The Power On/Off switch located on the unit, *unlike a standard PC*, does not directly shut off the power. Rather, it sends a power down request to the firmware. If the firmware is in the middle of an important operation, such as saving a vote, it will delay the power down until it is safe, unlike on a PC, where a power interruption during a file write operation can cause all sorts of havoc, including corruption of disk memory.

3) The AVC Edge® maintains an audit log, called the Event Log. This log is stored redundantly, on both the Audit Trail and Results Cartridge.

   Since all significant AVC Edge® events, including error conditions, are noted in this log, it is a valuable source of information on any anomalies that may have occurred.

Sequoia AVC Advantage Security Overview

Sequoia Voting Systems, Inc.
811 North Main Street, P.O. Box 1399, Jamestown, NY 14702-1399 (716) 487-0161

AVC ADVANTAGE®

SECURITY OVERVIEW

INTRODUCTION

Security is a blanket term which involves a variety of elements designed to mitigate potential risks and threats. In general, secure systems will control, through use of specific features, access to information such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.

The design of a secure environment involves the use of three types of *controls*:

Preventative Controls:

> The purpose of this type of control is to prevent the occurrence of one or more specific risks or threats. These controls can be use as a means of restricting or limiting access to data, functionality, or components. They may also be used to directly interdict potential threats or outside attack.

Detective Controls:

> All risks, threats, or attacks cannot be prevented — e.g., a system which permits outside dial-up access can use preventative control to stop unauthorized access, but it cannot prevent recurring attempts. In these cases, it is important to at least detect or record that such an event occurred. Detective controls are intended to identify real, potential, or attempted breaches in security. They are also often used to record an audit trail of activity which can be subsequently examined to identify potential problems or risks.

Corrective Controls:

> Even with preventative and detective controls in place, it is possible that damage or loss could occur (e.g., an authorized person uses such authorization to damage the system). Corrective controls are procedures or mechanisms which enable recovery from the loss or damage.

The security of any system, organization, or environment is not the result of merely one or two system components. It is the result of a variety of features, controls, architectural decisions, and procedures combining and building upon each other to produce a *security infrastructure*.

Security is fundamental to the election process. Security implies that the system must be reliable, it must accurately record votes and it must maintain the integrity of those votes. Security is achieved through features and controls which are inherent in the system design and through administrative controls. The acceptable level of security cannot be achieved with just one. Both types of controls must be present. This document is an overview of the security features and controls in the design of the AVC Advantage® central computer system and voting machines.

SYSTEM OVERVIEW

The AVC Advantage® Voting System is comprised of two major components, the AVC Advantage® Electronic Voting Machine and the Election Database System (EDS) Central System.

The voting machine incorporates two major components: the electronic voting machine (AVC) and the programmable memory device (Results Cartridge). The AVC incorporates a visual ballot surface, a voter selection panel that is capable of being properly aligned with the visual ballot surface, a control panel for use by election poll workers, appropriate electronic circuitry and processing devices for performing specified system functions, internal memory for storing ballot data and voting records, protective and public counters, and an enclosed voting booth for the purpose of voter privacy.

The Results Cartridge is designed so that it can be inserted into the voting machine, record voting results, be removed from the machine at the closing of the polls and be read by the EDS Central System. The Results Cartridge stores:

- an electronic representation of the ballot,
- ballot logic to enable the voter to make those selections to which he or she is lawfully entitled,
- the aggregated vote totals,
- randomized record of all individual ballots cast, and
- a chronological log of significant machine operations.

The EDS Central System ("EDS") is a computer software system which contains application software developed specifically for election requirements. The EDS System consists of the following subsystems:

- Election setup, which provides functions to initialize an election, define the political parties, offices and party positions, political subdivisions, types of elections and other global election variables.
- Candidate management, which allows the election office to identify the contests and candidates for an election.
- Ballot management, which provides for the layout of the visual ballots and the generation of the ballots in electronic or paper form.
- AVC management, which provides functions that helps manage AVC testing, maintenance and election preparation.
- Election results management, which provides the functions for election night tally of Results Cartridges and paper ballots (Absentee Ballots), the re-canvass of the election and the certification of all contests to the political parties and state election reporting agencies.

EDS DESIGN OVERVIEW

The primary security objective for the EDS design is to provide for controlled access to all system, application and database software and to be able to detect and report any unauthorized access to the system hardware and software. The accuracy of data entry and modification is also important and will be assured by system data verification checks and manual procedures. The data entry will be traceable by virtue of audit trails.

There are several procedural and physical steps that can be taken to secure the EDS System. One of these steps would be to see that all computers are kept in rooms secured by locks. Throughout the system all computers will employ several security features. Each PC can be physically secured by locks and seals on the PC chassis preventing introduction of unauthorized hardware or software elements. The diskette drives can be disabled to prevent the use of unauthorized software.

The software is also designed to limit access to only authorized users. Each user is limited in the functions that they can perform. Each program function verifies the user's security authorization before allowing access. Further, each user can be uniquely identified to the system. They should have their own ID and password. Passwords should be changed periodically. This reduces the likelihood and impact if a users password is discovered.

Password security includes other features. The system has a function that will enable and disable system wide security authorizations for the functions that may be accessed. For instance, on election day functions that could modify the ballot would be disabled and on election night, all AVC functions other than vote tally could be disabled.

The EDS has an audit trail that records actions and events within the system. This audit trail includes:

- successful log on and log off,
- unsuccessful log on attempts,
- attempts to violate security,
- history of user action,
- changes to security authorizations,
- system access violations.

Where practical, the audit trail identifies the user, date, time and the description of the event being recorded.

Physical security is also important for EDS. Limiting access to the EDS computer, by keeping it in a locked room for example, is also recommended.

AVC DESIGN OVERVIEW

Fourteen years ago, when the AVC was developed, security & integrity of the voting process were cornerstones of the design philosophy. The design has several key features that enhance system security and maximize resistance to virus and Trojan horse type attacks. These will be discussed in more detail below.

Careful consideration was also given to the *longevity* of the design. This led to the choice of the Z80 microprocessor, a tried & true, and very capable device. It is still being sold today by the millions, *some twenty years after it was designed.* Can any of the PC microprocessors (8088, 80286, etc.) make this claim? This is important, because it assures our customers that the new machines they buy will be compatible with the ones they have had for years, that spare parts & service are available (try getting service or parts for an IBM XT, for comparison).

Finally, the *reliability* of the system was designed to be very high. In ten years, with over 12,000 AVCs in use, in countless elections and with countless numbers of votes cast, *not a single vote has been lost to equipment malfunction.*

Were the design goals met? Yes, in spades. The security of the AVC has been studied in depth by several independent organizations, including SRI International and Wyle Labs. The AVC has been certified for use in over 20 states (and still counting). The only significant change to the electronics in that time has been to increase the amount of memory in the system, both for more complex ballots, and to add new voting features.

AVC SECURITY

It is helpful to look at *where* in an election cycle attacks could be mounted, so that there is a context for the security features in the system. Where can attacks be made?

- During development of the AVC's software.
- During ballot definition and cartridge generation at EDS.
- During transport of programmed Results Cartridges to the AVC warehouse.
- During the AVC technician's Ballot Verify and Pre-LAT process.
- During the Election.
- During transport of the Results Cartridges to the tally site.
- During tally at EDS.

In a similar vein, the results of attacks on the election cycle can be broadly categorized as:

- Denial of Service
- Alteration of Vote Data

Denial of Service attacks, which might typically be of a vandalism nature, are an equal threat to all voting systems, electronic or paper based. Alteration of Vote Data attacks (or the loss of vote data) are of more importance; the sections that follow will describe the safeguards in the AVC that make such attacks closer to impossible on the AVC than with any other voting system.

One important point to also keep in mind is that a *meaningful* attack, in either category, must involve affecting a large number of votes. After programmed Results Cartridges leave EDS, they move into the hands of *several* AVC technicians for machine preparation, and on election day, the AVCs are in the hands of *hundreds* of poll workers, at multiple physical locations. Collusion at this level is unlikely to go undetected.

Security features within EDS were described earlier; the following discussion will focus on security features within the AVC.

Loading the Ballot Onto the AVC

Each AVC must go through a process called Ballot Verify to load the EDS-defined ballot. It must then also go through a Pre-Election Logic & Accuracy Test (Pre-LAT). It is not possible to bypass these steps.

The Ballot Verify and Pre-LAT operations are typically performed by AVC technicians, with the AVCs still in the storage warehouse. These operations are preceded by attaching the printed ballot face to the AVC.

When EDS generates a ballot and loads it onto a Results Cartridge, it provides several levels of integrity checks for the AVC:

- Each Results Cartridge is “branded” with the destination AVC’s serial number.
- A CRC is calculated for each of the ten basic data files that comprise the ballot definition. These CRC values are stored along with the ballot data.
- A cryptographic signature of all the files on the results cartridge is generated and stored in the cartridge, separate from the ballot definition data.

The cryptographic signature mentioned above uses an algorithm that was developed in consultation with RSA Data Security, Inc., a leading encryption provider. This algorithm is “seeded” with a value that is stored in a special non-volatile ROM (Read-Only Memory) in the AVC; the only way to discover or change this value is to physically remove the ROM from the AVC.

During Ballot Verify the AVC initializes itself for the upcoming election based on the ballot files read from the Results Cartridge. To conduct Ballot Verify, a Results Cartridge must be inserted in the AVC. The ballot definition on the Results Cartridge is subjected to the following tests before it is loaded into the AVC:

- The serial number on the Results Cartridge must match this AVC.
- The cryptographic signature calculated & stored by EDS is validated.
- The ballot file CRC values calculated & stored by EDS are validated.
- Make sure there is no vote data already stored on the cartridge, of any type: Ballot images, write in names, candidate totals counters and selection code totals counters.

Any failure in the above tests will cause the AVC to declare an error, and it will the reject the Results Cartridge. From this point forward the AVC will not operate without the correct Results Cartridge installed.

The next step in Ballot Verify is for the AVC technician to confirm that the logical ballot definition in the AVC matches the visual ballot seen on the voter panel. All vote positions, vote for numbers, contest headers, and candidate types, for each selection code (e.g. each ballot subset) are validated by the Technician. The AVC also generates a report verifying the completion of this step and finally provides a printed ballot definition report of the electronic ballot.

The Pre-Election Logic and Accuracy Test (Pre-LAT) verifies the logical correctness of the ballot and its match to the visual ballot. During this test all activity is the same as it would be in an official election and the same software logic is exercised, with the important exception that the vote data is stored separately from the Official Election vote data.

Voting during Pre-LAT can be either manual, or automatic via a vote simulation script. This vote simulation feature, which is only available in Pre-LAT, allows the ballot logic to be tested, with large numbers of votes (in excess of 50,000 keystrokes), and without the possibility of data entry errors.

Upon closing of the polls, the AVC prints a Pre-LAT results report and the totals can be compared to the predicted totals from manual or Vote Simulation scripts.

Conducting the Election

During the Election, the Results Cartridge must always be inserted in its port. If it is removed, the AVC will stop its normal operations, generate an error indication and make an entry in the Operator Log. In addition, the Auxiliary Port must be kept empty. Attempting to insert *any* cartridge type into this port will also stop normal operations, generate an error condition and make an Operator Log entry.

Means are provided to use a numbered seal to physically ensure that the Results Cartridge is not removed.

At the opening of the polls, a zero proof report is generated which includes the AVC poll site, precinct number, public counter and protective counter, and all ballot information with the state of the internal vote counters. This report proves to the poll site officials that the AVC has no previously stored vote data.

The process for recording votes includes the use of redundant memories, one resident on the CPU board in the AVC, and the other in the Results Cartridge. These memories are verified to be identical after each voter is finished, and also each time the AVC is turned on while in

Election Mode. Any error or mismatch in the verification process will generate an orderly shutdown and an error message.

The vote recording process begins when the voter presses CAST VOTE. The booth light and voter panel lights are turned off and the cast vote song is played. The Election Program then composes the voter's Ballot Image record and increments the totals counter of each candidate that the voter selected. A CRC value is calculated and appended to each Ballot Image. This data is saved to both the Audit Trail memory on the CPU board and the Results Cartridge. All operations are double-checked (reading back data just written, etc.) during the vote saving process. After all the voter data is stored the public and protective counters are incremented. Any error that may occur during the vote save process is uniquely reported and causes the voting process to stop on this AVC.

The AVC then performs an internal cross-check of the redundant memory areas (Audit Trail and Results Cartridge). This cross-check makes sure the two memories are identical, down to the bit level; it includes the vote totals and ballot image storage areas. Any discrepancy is cause for halting the voting process on this AVC. Next, an internal "recount" is performed. This recount validates each ballot image and recalculates the summary totals from the ballot image data. Any mismatch between the ballot image totals and the summary totals counters will be detected. After a successful cross-check, the poll worker may activate the machine for the next voter.

> Note that the Audit Trail memory and Results Cartridge memory have independent battery backups. In keeping with the design longevity goal, these batteries are standard AA cells. A fresh set of batteries will last for several years. The health of these batteries is checked several times *each second* by a background firmware process. If either battery's voltage falls too low, the AVC will stop normal operations, generate an error condition and make an Operator Log entry. The voltage where the error is announced has been verified to still provide several *weeks* of battery life - more than enough time to handle all tally and post-election functions.
>
> It should also be noted that, while the AVC is turned on, there is no drain on these batteries - the main power source takes over.

Since the AVC retains a ballot image record for each voter, it is important that these ballot images not be saved in the order in which they were cast as that would provide the ability to learn how an individual cast their vote. When the AVC allocates storage space for ballot images and write-in data, it takes the following steps to assure storage of this data is sufficiently random to avoid identification of voter data with individual voters.

1) Storage space is allocated in large blocks rather than on a per-voter bases. When an allocation is required, a random number of storage blocks between 25 and 50 are allocated.

2) Access to the storage blocks is via an indirect table of block numbers. This table is shuffled randomly when the blocks are allocated, so that the sequence of storing ballot images within the storage blocks is random.

The randomizing function in the AVC uses a mathematical pseudo-random number generator that is further randomized by the value of the AVC's internal real time clock at the time of the random number request. This pseudo-random number generator has been reviewed by independent computer experts and been deemed sufficiently random that it would not reasonably be reversible based on the amount of data that would serve as the basis for the reversal.

Tallying Results

After polls are closed, the AVC immediately calculates and stores cryptographic signatures of each of the totals data files (ballot images, write in names, candidate summary totals, and selection code summary totals). The cryptographic signature values are stored in both the Audit Trail and Results Cartridge memories. The cryptographic signature algorithm is the same one that validates the integrity of the ballot definition, described earlier.

Next, the AVC prints a Results Report. This report shows the value of each candidate counter (including ballot measures) and also shows voter turnout data per precinct or primary party, if applicable.

Once the report is complete, the Results Cartridge can be removed and transported to the EDS system for tally. Typically, this transport is done in a secure manner - the cartridges are placed in a sealed case and transported by at least two poll workers.

Once at EDS, the cartridges are tallied. EDS validates the ballot definition on the cartridge to make sure the cartridge has come from the correct election definition. Cartridges that have an incorrect ballot are rejected. EDS also maintains lists of cartridges that were assigned to this election, and of cartridges that have already been tallied. Each time a Results Cartridge is presented for tally, it is checked against these lists.

If a question arises about the integrity or accuracy of the election night tally, several safeguards can be relied upon:

- The cryptographic signatures of the totals information can be re-validated.
- There is still a redundant copy of the vote data, and ballot, on each AVC. An AVC’s Results Cartridge can be returned to the AVC, and the two copies verified to still match.
- The data that EDS tallied from the Results Cartridge can be verified against the Results Report printed by the AVC when polls closed.
- EDS can print data directly from a Results Cartridge. Results Reports, Ballot Image details, and the Operator Log can all be printed.

- Additional copies of the Results Report can be printed from the AVC's Audit Trail memory.
- The AVC's Operator Log can be printed at the AVC.
- The AVC can generate an Audit Trail report with ballot image details.
- The AVC provides a function to directly review candidate totals on the machine, by pressing candidate positions on the voter panel. (This function is only available *after* polls have closed.)

What would happen if a Results Cartridge were lost, or damaged while in transit to EDS for tally?

There are two methods of dealing with this situation. The first is to use EDS to manually enter the vote data for the AVC, from the printed Results Report. The second method is to use a special "Audit Trail Transfer" Cartridge. This cartridge, in conjunction with a firmware function only available at polls closed, allows for transferring an exact copy of the AVC's Audit Trail memory to the cartridge. EDS can then do its tally from this cartridge. Finally, additional copies of the Results Report can be printed from the AVC's Audit Trail memory.

EARLY VOTING

Early voting presents a new set of security challenges. The AVC implements Early Voting as a number of "sessions" within the Polls Open state. In use, each Early Voting session corresponds to one day (or other period) of Early Voting.

At the end of an Early Voting session, the AVC must be secured from further voting. This is done by entering a "lock" mode. To enter the lock mode, the vote data from the session being ended is transferred to a special Early Voting cartridge. Cryptographic signatures, using the algorithm discussed earlier, protect this vote data from alteration. The only report that is printed at the end of a session is a "turnout" report that shows the number of voters per precinct.

The Early Voting cartridge is transported to EDS, where it is validated, and then saved in an encrypted format, using Triple-DES. Multiple copies of the data are saved, typically on different physical storage media, to protect against equipment failures. EDS also makes entries in an event log on the Early Voting cartridge (protected by another cryptographic signature) to indicate that the data was collected successfully.

When it is time to open a new voting session, the Early Voting cartridge is once again presented to the AVC. The AVC verifies that the proper log entries have been made, and that the cryptographic signatures are correct. Once this is done, the vote data from the previous session are cleared and the AVC moves to an unlocked state, ready for voting in the new session.

Closing polls, after all Early Voting sessions are complete, can only be done from the lock mode. It is only at this time that a grand total results report, that spans all sessions, is available for printing. Note that this report is not printed automatically; the command to print the report is in a post-election menu that poll site workers do not have access to.

At EDS, nothing can happen to the encrypted vote data from each session *until* the results cartridges from the AVC are read to verify that polls are in fact now closed. It is only at that point that the vote data can be decrypted (after validating that the multiply saved copies are identical) and tallied.

Isn't There a Lot of Risk Here?

There's no doubt that Early Voting is a more complex process than a typical Official Election. Great pains have been taken to make Early Voting "more secure than Ft. Knox".

At the AVC, the following precautions are in place:

- All data copied to the Early Voting cartridge is protected by the cryptographic signatures.
- Backup copies of the candidate counters and selection code counters for each session are saved in both the Audit Trail and Results Cartridge, again protected by cryptographic signatures.
- Several independent indications, including cryptographic signatures, must be present on the Early Voting cartridge before the AVC is satisfied that the previous session's data has been successfully saved and it is safe to prepare for the new session.

At EDS, the following precautions are in place:

- The validity checking of the Early Voting cartridge before accepting data from it is more extensive than for Election Night processing.
- Data is encrypted with Triple-DES (112 bit effective password length), and saved to a minimum of two locations, which are typically two different disk drives, or even two separate computers (networked).
- Each AVC's results Cartridge must be read, and a valid polls close event log event found, before any of the session data can be tallied.
- Before decrypting and processing the data, the multiple copies are compared; they must be identical.

Finally, there are provisions, in both the AVC and EDS, for recovery from a bad or misplaced Early Voting cartridge.

OTHER POINTS AND ISSUES

Can Malicious Software Be Introduced Into the AVC?

No. Here are the reasons why:

In order to verify that the correct firmware is installed in each machine, Sequoia has administrative controls in place from the time the firmware is written and compiled until the time it is locked and sealed in each AVC. The points in this sequence are when:

- The firmware is written and the master program ROM created,
- The master ROM is reproduced for installation in each AVC, and
- The AVCs are delivered to a customer.

The AVC firmware is written in a high level language and is well designed and written so that it can be easily read and understood. This has been confirmed by several independent reviews of the source code, and by the FEC certification process. Sequoia conducts comprehensive testing as part of the qualification acceptance testing of the AVC. Various versions of the firmware have been certified in over 20 States.

The AVC software is under strict configuration management control. This means that there are verifiable means of controlling, accounting for, and verifying any and all changes to the baseline machine firmware, which has been the subject of detailed review. The firmware is compiled twice, by different people, on different computers and the results verified to be equivalent.

During the assembly of the AVC there are manufacturing controls to provide assurances that the correct version of firmware is being installed in each machine. Also in manufacturing there are procedures that allow SPVE to verify that the known version of software is, in fact, the version installed on the AVCs.

Each machine is a stand alone processor. Errors cannot be promulgated from one machine to another. The machines cannot be accessed by telecommunications. The vote counting instructions in each voting machine are written into integrated circuit chips during the manufacturing process. These chips are incorporated into each machine's circuit boards. Access to the machine should be limited by administrative procedures and is also limited by the physical design of the machines. Design features include door locks and a numbered seal on the CPU cover.

Finally, malicious program code cannot be introduced into the AVC through the Results Cartridge. The machine's electronic design and the design of the microprocessor itself renders it impossible to execute instructions from the Results Cartridge or any area other than the program chips. If this is attempted the machine displays an error message and halts.

There are three scenarios for how instructions could be introduced into the AVC through the Results Cartridge. They are:

1) Data in the Results Cartridge triggers a malicious section of code within the AVC,
2) Code is downloaded from the Results Cartridge to RAM and then executed, and
3) Code is executed directly from the Results Cartridge.

The first scenario is protected against by the controls over the AVC firmware discussed above. The remaining scenarios require some background on the AVC design.

The microprocessor in the AVC is the Z80. The Z80 has 64K of addressable memory. Of this addressable memory, the AVC's circuit design designates the first half of this memory (32K) as ROM, Read Only Memory. This ROM contains the AVC program instructions, or firmware. The ROMs cannot be cannot be changed without removal from the system. The second 32K of addressable memory contains RAM, random access memory.

The design of the Z80 and the electronics of the AVC do not physically allow data to be read from this RAM and executed as instructions. In addition, were this to happen, the AVC circuitry is designed to stop the program execution, generate an error message and automatically shut down. Hence, no data in the AVC RAM could be executed as an instruction.

The Z80 provides a positive indication of every time memory is accessed to get an instruction to be executed. (Instructions are first read into the Z80, then acted upon.) The AVC electronics uses this "instruction read" indication to check that the Z80 is indeed attempting to read the instruction from one of the firmware chips. If this is not the case, there will be two preventative responses, both of which are part of the AVC's circuitry, so cannot be overridden by software.

1) The Z80 is isolated from the rest of the AVC so that the instruction that was requested never makes it to the Z80. This is done by disabling the system's data bus.

2) A "break" signal, or non maskable interrupt, is generated for the Z80 that forces the Z80 to execute a special firmware function that displays "Opcode fetch from RAM" and halts the AVC. This break signal is generated in such a way that, by the design of the Z80, it cannot be ignored by the Z80. (And if, for some reason, another "instruction read" from other than the firmware chips was attempted while processing the first error, the whole process would repeat.)

Hence, the AVC cannot execute instructions from RAM. *Keep in mind that PC's, whether running DOS or Windows or any other Operating System, are vulnerable to viruses precisely because they load executable code into RAM.*

The AVC also cannot execute instructions directly from the Results or Auxiliary Port. The AVC is designed so that these ports can only be accessed in the Z80 input/output mode. Devices defined in this way are physically limited by the Z80 construction to allow only data reads and writes. The Z80 cannot retrieve an instruction from any peripheral device designed to be in input/output area. Only data reads and writes can occur in this mode; the Z80's internal design prevents the possibility of code execution. The AVC uses this access mode exclusively for the Results and Auxiliary Ports; the AVC electronics design is such that the Z80 cannot access them any other way.

In summary, there are controls from the source code review through the manufacture and delivery of the AVC to protect the integrity of the program ROMs. Thereafter, the AVC design limits access to the program ROMs through physical means -- locks and seals -- and logical means -- checksums at power up and program initiation. Finally, by machine design the machine is not accessible to the outside except through the Results Cartridges. The AVC and its microprocessor have design features that restrict the ability to execute instructions from RAM or from the Results Cartridge.

Other AVC Security Features

1. The AVC has locks on both the Voter Panel and the rear door. The rear door provides access to the cartridge ports, and also to the cover of the CPU board.

2. The AVC is designed to allow the attachment of seals to its various parts to ensure that there is no unauthorized access. These seals are typically serialized, and recorded on election paperwork, and they cannot be removed without destroying them. Also, the cartridges cannot be taken apart without physically damaging the cartridge label, providing additional evidence of tampering.

3. The AVC uses a software-controlled power down. The Power On/Off switch located on the unit, *unlike a standard PC*, does not directly shut off the power. Rather, it sends a power down request to the firmware. If the firmware is in the middle of an important operation, such as saving a vote, it will delay the power down until it is safe, unlike on a PC, where a power interruption during a file write operation can cause all sorts of havoc, including corruption of disk memory.

Before powering down, the AVC performs additional “housekeeping” tasks, such as redundantly saving areas of battery backed memory that are especially critical (such as the current election mode indicator).

4. The AVC’s firmware is subject to multiple validations during the course of normal operations:
   - Checksums of each firmware ROM and the Configuration ROM are stored in battery-backed-up system RAM. At each AVC power up, these checksums are re-calculated and compared to the stored values. A change in checksum values will cause a power up error to be indicated, an informational report to be printed, and a "checksum changed" event to be logged to the maintenance log. A separate report is generated for each of the individual ROMs.
   - The AVC Operating System and each of the individual application programs is stored in ROM with a checksum. Each time the AVC powers up, it verifies each of these checksums. If any checksum fails to match the value stored in ROM, the AVC will generate an error message, print a report, log the event and then halt. Before loading and executing an application program, its checksum is again verified. If there is a mismatch, the AVC will generate an error message, print a report, log the event and then halt.

5. The AVC has been tested for correct operation in the presence of extreme electromagnetic fields. These tests included:

- Continuous modulated electromagnetic fields with an electric field intensity of 10 V/m with a frequencies between 2 MHz and 1 GHz,
- Continuous unmodulated electromagnetic fields within the frequency range of 0.1 MHz to 1000 MHz with a field intensity of 200 V/m,
- Pulsed unmodulated electromagnetic fields with field strength up to 200 V/m at frequencies between 2-10 Ghz.

To put these numbers in perspective, it is *unsafe* for a person to be in the test chamber with the AVC while the strongest of these fields is present.

6. The AVC maintains an event log, called the Operator Log. This log is stored redundantly, on both the Audit Trail and Results Cartridge. It can be printed out after polls are closed, both at the AVC (for the Audit Trail copy) and at EDS (the Results Cartridge copy).

   Since all significant AVC events, including error conditions, are noted in this log, it is a valuable source of information on any anomalies that may have occurred.

7. If, despite all the above safeties and precautions that have been discussed, the processor still "crashes", the following safeguard takes over:

   Unlike a standard PC, the AVC's CPU board includes a feature called a "watchdog timer". This must be reset at least once per second, or it will generate a "break" signal to the processor. The processor cannot ignore this "break". The normal system operation ensures that the watchdog timer is reset many times per second.

   If the processor were to "crash", the watchdog's "break" signal will bring the AVC's CPU back under control.

Methods of Recounting Electronic Ballots

SEQUOIA
voting systems

Five Ways to Perform Recounts on Electronic Voting Systems

1. Re-tabulate the result cartridges from each voting machine.

2. Create audit trail cartridges from each voting machine using the data retained in the touch screen unit's internal memory. Re-tabulate the results using the data copied from the touch screen's redundant memory storage.

3. Recount the summary of results that are printed by each voting machine at the close of the polls and compare them to the accumulated totals in the central database.

4. Touch screens store an electronic "image" of each voter's ballot. The ballot image can be printed on the printers attached to each touch screen. A manual hand recount of these images can be conducted.

5. Touch screens store an electronic "image" of each voter's ballot. The ballot image can be printed from a workstation connected to the results cartridge readers. A manual hand recount of these images can be conducted.

Two Additional Ways to Recount Votes on Electronic Voting Systems with Voter Verifiable Paper Records

1. Ballot images can be printed on paper behind glass for voters to review and accept. These secure records retained inside in the voting machine can be manually recounted or used as an additional audit tool to verify accuracy.

2. If properly equipped, a high-speed machine scan/recount of the voter verified paper ballot images can also be conducted.

* *Direct recording electronic voting equipment manufactured by Sequoia Voting Systems currently accommodates five methods of conducting recounts. With our patent-pending VeriVote® printer upgrade, Sequoia will also offer voters the opportunity to review and verify a printed record of their votes before leaving the voting booth. These additional paper records can be used to permit two additional methods of recounting ballots.*

Sample Electronic Ballot Image Printout

```
***********************************
  PRE-LAT FULL AUDIT*TRAIL REPORT
***********************************

Date 01/16/2004           Time 02:10 PM

Serial Number                     10342

Protective Counter                10626

Public Counter                        3

Poll Site
  PCT 1313

Polling Place ID                     01

Ballot Version                        0

Report Source          Cartridge Memory

  Demonstration Election



   Pre Election LAT Summary Totals

Governor                          (1)
  REINHOLD GULKE                      1
    American Independent
  GRAY DAVIS                          0
    Democratic
  IRIS ADAM                           1
    Natural Law
  PETER MIGUEL CAMEJO                 0
    Green
  GARY DAVID COPELAND                 0
    Libertarian
  BILL SIMON                          0
    Republican
  Write-In                            0


Lieutenant Governor               (1)
  PAUL JERRY HANNOSH                  1
    Reform
```

```
      BRUCE MC PHERSON                    0
        Republican
      KALEE PRZYBYLAK                     0
        Natural Law
      CRUZ M. BUSTAMANTE                  0
        Democratic
      JIM KING                            0
        American Independent
      DONNA J. WARREN                     0
        Green
      PAT WRIGHT                          0
        Libertarian
      Write-In                            0


    Secretary Of State                (1)
      EDWARD C. NOONAN                    1
        American Independent
      LOUISE MARIE ALLISON                0
        Natural Law
      KEITH OLBERG                        0
        Republican
      KEVIN SHELLEY                       0
        Democratic
      VALLI SHARPE-GEISLER                0
        Reform
      LARRY SHOUP                         0
        Green
      GAIL K. LIGHTFOOT                   0
        Libertarian
      Write-In                            0


    Treasurer                         (1)
      SYLVIA VALENTINE                    1
        Natural Law
      NATHAN E. JOHNSON                   0
        American Independent
      PHIL ANGELIDES                      0
        Democratic
      GREG CONLON                         0
        Republican
      MARIAN SMITHSON                     0
        Libertarian
      JEANNE ROSENMEIER                   0
        Green
      Write-In                            0
```

```
Attorney General                  (1)
  GLEN FREEMAN MOWRER                 1
    Green
  ED KUWATCH                          0
    Libertarian
  DICK ACKERMAN                       0
    Republican
  DIANE BEALL TEMPLIN                 0
    American Independent
  BILL LOCKYER                        0
    Democratic
  Write-In                            0


16th Congressional Dist.          (1)
  DOUGLAS ADAMS                       1
    Republican
  DENNIS UMPHRESS                     0
    Libertarian
  ZOE LOFGREN                         0
    Democratic
  Write-In                            0


23rd Assembly District            (1)
  WARNER S. BLOOMBERG                 1
    Green
  MANNY DIAZ                          0
    Democratic
  Write-In                            0


STATE PROPOSITION 46              (1)
  YES                                 1

  NO                                  0


STATE PROPOSITION 47              (1)
  YES                                 1

  NO                                  0
```

Pre Election LAT Audit*Trail Record

```
  Standard votes
```

```
   60           72           79
    91           98           118
    124          474          476

   63

  No Selections Made
```

Write In Votes

No Write-In Votes in Memory.

63

Audit*Trail Totals

Governor	**(1)**
REINHOLD GULKE	1
American Independent	
GRAY DAVIS	0
Democratic	
IRIS ADAM	1
Natural Law	
PETER MIGUEL CAMEJO	0
Green	
GARY DAVID COPELAND	0
Libertarian	
BILL SIMON	0
Republican	
Write-In	0

Lieutenant Governor	**(1)**
PAUL JERRY HANNOSH	1
Reform	
BRUCE MC PHERSON	0
Republican	
KALEE PRZYBYLAK	0
Natural Law	
CRUZ M. BUSTAMANTE	0
Democratic	
JIM KING	0
American Independent	
DONNA J. WARREN	0
Green	
PAT WRIGHT	0
Libertarian	
Write-In	0

Secretary Of State	**(1)**
EDWARD C. NOONAN	1
American Independent	
LOUISE MARIE ALLISON	0
Natural Law	
KEITH OLBERG	0
Republican	
KEVIN SHELLEY	0
Democratic	
VALLI SHARPE-GEISLER	0
Reform	
LARRY SHOUP	0
Green	
GAIL K. LIGHTFOOT	0
Libertarian	
Write-In	0

Treasurer	**(1)**
SYLVIA VALENTINE	1
Natural Law	
NATHAN E. JOHNSON	0
American Independent	
PHIL ANGELIDES	0
Democratic	
GREG CONLON	0
Republican	
MARIAN SMITHSON	0
Libertarian	
JEANNE ROSENMEIER	0
Green	
Write-In	0

Attorney General	**(1)**
GLEN FREEMAN MOWRER	1
Green	
ED KUWATCH	0
Libertarian	
DICK ACKERMAN	0
Republican	
DIANE BEALL TEMPLIN	0
American Independent	
BILL LOCKYER	0
Democratic	
Write-In	0

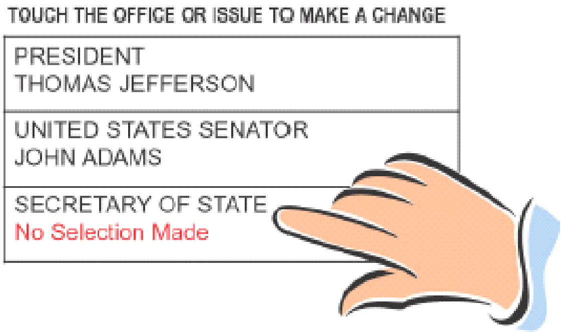
```
16th Congressional Dist.          (1)
  DOUGLAS ADAMS                       1
    Republican
  DENNIS UMPHRESS                     0
    Libertarian
  ZOE LOFGREN                         0
    Democratic
  Write-In                            0


23rd Assembly District            (1)
  WARNER S. BLOOMBERG                 1
    Green
  MANNY DIAZ                          0
    Democratic
  Write-In                            0


STATE PROPOSITION 46              (1)
  YES                                 1

  NO                                  0


STATE PROPOSITION 47              (1)
  YES                                 1

  NO                                  0
```

Verifying Technician

Undervote Warning Messages on Sequoia AVC Edge Touch Screen

Automatic Review Screen

After pressing the Next button on the last page of the ballot, the review screen will automatically be displayed. It will list by contest, only the candidate(s) or choices currently made by the voter. This allows the voter to review on one page, all of their choices prior to casting the ballot.



TOUCH THE OFFICE OR ISSUE TO MAKE A CHANGE

PRESIDENT
THOMAS JEFFERSON

UNITED STATES SENATOR
JOHN ADAMS

SECRETARY OF STATE
No Selection Made

Contests that have not been fully voted are displayed in a bold highlight. If the voter wishes to make a change, touching the desired contest will automatically display the appropriate page of the ballot. The voter can now make a different selection.

Undervote Warning

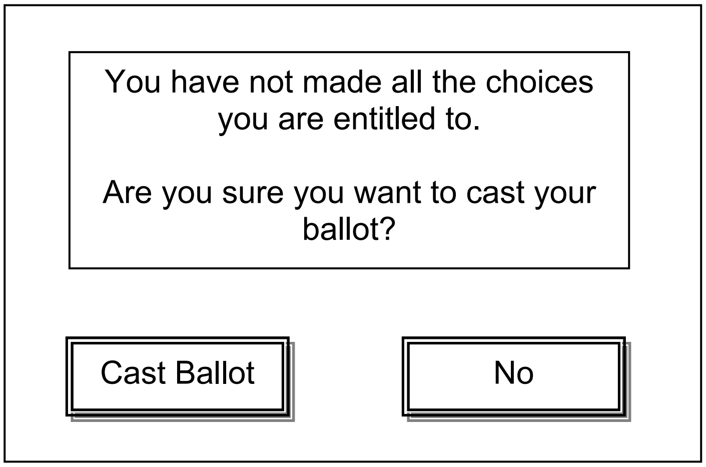
If the voter has not made all of the selection(s) that they are entitled to on the ballot, a warning message will be presented on the Cast Ballot page:

You have not made all the choices you are entitled to. Press Back to return to the Ballot.

This warning is to help prevent the voter from accidentally casting a ballot that has been undervoted. Pressing the Back button will allow the voter to return to the ballot for any necessary changes.

Undervote Confirmation

If the voter has not made all of the selection(s) that they are entitled to on the ballot and touches the Cast Vote button, the following warning message is presented:



You have not made all the choices you are entitled to.

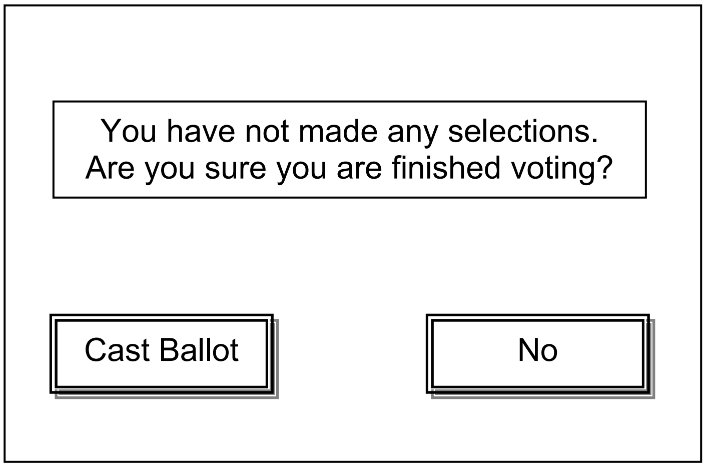
Are you sure you want to cast your ballot?

This warning is to help prevent the voter from accidentally casting a ballot that has been undervoted.

If the voter wishes to go back and check the ballot, touching the No button will return them to the cast ballot page. If the voter wishes to continue casting the ballot, touching the Cast Ballot button will cast the undervoted ballot.

Blank Ballot Warning

If the voter has not made any selection(s) on the ballot and touches the Cast Vote button, the following warning message is displayed:



You have not made any selections.
Are you sure you are finished voting?

This warning is to help prevent the voter from accidentally casting a blank ballot. If the voter wishes to go back and check the ballot, touching the No button will return them to the cast ballot page. If the voter wishes to continue casting the ballot, touching the Cast Ballot button will cast the blank ballot.

Sequoia Press Release Announcing Intention to Offer Voter Verifiable Paper Record Printers

FOR IMMEDIATE RELEASE Contact: Alfie Charles
Friday, November 21, 2003 916-683-4525

Sequoia Voting Systems Announces Plan to Market Optional Voter Verifiable Paper Record Printers for Touch Screens in 2004

Would Enable Electronic Ballots to Be Printed for
Voter Review and Acceptance at the Polls

Oakland, CA – Sequoia Voting Systems, one of the nation's largest suppliers of election equipment and services, announced today that it will formally seek federal certification of its unique voter verifiable paper record printer as an optional component to the company's AVC Edge® touch screen voting system. The new product upgrade will be submitted for federal testing in the first quarter of 2004.

"Our customers routinely praise our system's ease of use for voters, poll workers and election officials," said Sequoia President Tracey Graham. "Voting on the Sequoia touch screens will remain as easy as ever, but with this additional feature, voters will have the added convenience of viewing a paper record of their selections before they leave the polls."

"While our existing electronic voting equipment already allows the printing of ballots for recount and audit purposes, this new feature will allow each voter to confirm their selections both electronically and on paper," noted Graham.

The printer will be mounted beside the touch screen and will display the voter's selections behind glass so voters will not be able to physically handle, remove or alter the paper. After the voter confirms that the selections on the paper are correct, they will then officially submit their ballot via the touch screen. After the ballot is cast, the paper record is scrolled inside the unit to maintain a voter verified paper audit trail.

The additional paper audit trail will supplement existing features such as the system's redundantly stored electronic ballot images and unalterable electronic audit logs to provide multiple methods of verifying the accuracy of an election.

The new feature is optional and is not required to ensure the integrity of electronic ballots. The enhanced printer option can be added to any existing or new Sequoia AVC Edge touch screen voting units in the market. The option can be implemented at the time of purchase or can be added at a later date if state or local election requirements change.

Electronic voting systems are closely regulated by federal and state officials. Both the hardware and software of electronic voting systems must be tested

7677 Oakport Street
Suite 800
Oakland, CA 94621
t:510.875.1200
t:800.869.1936
f:510.875.1209
www.sequoiavote.com

against more than 500 pages of standards and requirements by federally sanctioned independent testing authorities.

Sequoia's touch screen voting units were first used on a countywide basis for the historic 2000 presidential elections conducted by Riverside County, California. On October 7, 2003, the system was deployed ahead of schedule in Shasta County, California so voters there could take advantage of the new technology during the complex California Gubernatorial Recall election.

Sequoia Voting Systems provides election services in more than thirty-five states and has more than 48,000 electronic voting machines deployed across the nation. Sequoia has been providing election services for more than a century and electronic voting machines for 25 years. The touch screen version of Sequoia's electronic voting equipment has been available since 1999.

Sequoia is based in Oakland, California with offices in Colorado, Florida and New York. Sequoia has led the election services industry by providing direct recording electronic voting systems for the last twenty-five years. Sequoia is a subsidiary of De La Rue, PLC, a global leader in providing tamperproof government documents and secure cash handling and processing technologies.

Security Analysis by
State of Nevada
Gaming Control Board

MEMORANDUM

Date: November 26, 2003

To: Dean Heller, Secretary of State

From: Marc McDermott, Chief
Electronic Services Division

Subject: Diebold and Sequoia Voting Machine Security

Summary

I believe the Diebold electronic voting machine, operating on the software analyzed in the Johns Hopkins report and the SAIC Risk Assessment Report, represents a legitimate threat to the integrity of the election process. Conversely, based on available information with regard to the Sequoia Voting System, I believe the Sequoia electronic voting machine represents a much more secure option because of the increased security of the customer (voter) interface and by the fact that the Sequoia operating software has not been made available on the Internet.

Supporting Information

I reviewed the information supplied with your letter of October 2, 2003 regarding an analysis (the Johns Hopkins report) of Diebold electronic voting machines. This analysis, written by personnel from the Information Security Institute of Johns Hopkins University and the Department of Computer Science of Rice University, was based on Diebold electronic voting machine software that had been put on the Internet. The analysis pointed out numerous security problems and areas of vulnerability with the Diebold machines. Unfortunately, after reviewing the report, I would agree with the report's findings and believe that the majority of the problems listed are valid.

Based on my experience in counter-terrorism and as Chief of the Gaming Control Board's Electronic Services Division, I believe the primary target for a hacker would be the voter interface. At these points, the public comes into physical contact with the voting machines. If someone wanted to attack a voting machine, the normal voting process would allow this person access to a machine for several minutes. During this time, when he was supposed to be voting, the attacker could try to gain entry to the machine's software to either change how the machine operates or change the stored voter information. The only interfaces or data entry points available to the attacker at this time are the touch screen and the smart card reader. Of these, only the smart card reader provides a reasonable path to get deep enough into the voting machine's operating software to pose a threat to the machine. It is in this critical interface that the Diebold and Sequoia machines differ significantly. According to the Johns Hopkins report, the Diebold machines send and accept data from the smart card reader in plain, unencrypted text. I agree with the Johns Hopkins report's conclusion that this is a poor choice. As explained on pages 11 and 12 of that report, the clear-text messages allow for a compromise of both the administrative password and the password used to authenticate the terminal to the smart card. As a result, I believe that the availability of smart cards, smart card readers and smart card development tools, combined with both the Diebold software and the Johns Hopkins report on the Internet, represent a real threat to any election using the Diebold machines.

Conversely, the Sequoia machine provides basic encryption of the information sent between the smart card and the voting machine. This reason alone would be enough to recommend the Sequoia over the Diebold system, as I would see an obvious flaw such as sending unencrypted data to the smart card as indicative of other serious security issues. However, in addition to a software security concern, Diebold's source code for their voting machine was put on the Internet. This immediately raises many questions regarding the security of the entire Diebold software development and management process. There should be very tight internal controls for software development of this kind. Since this information got to the Internet, it casts a shadow of uncertainty on the security consciousness of the entire development team.

The Diebold system has been evaluated by Johns Hopkins and SAIC and both evaluations have indicated serious security deficiencies. However, as stated in the SAIC report, when taken in the context of a real election, the internal controls governing the election will greatly reduce or completely eliminate the majority of the deficiencies found. For example, if a password for a voting terminal is extracted and fake smart cards are made, they would only be valid on one particular voting machine. At a polling place, voting officials, not voters, choose what terminal a voter is to use. As there are many voting terminals at most polling places, many fake cards would be necessary and would have to be distributed to many confederates hoping that one would be assigned to the terminal where the card would work. Additionally, there is a very good chance that any errors such as extra votes or other irregularities caused by these fake cards would be detected after the polls closed and the votes were tallied. The problem is that, if even one fake card was shown to work, even if it was discovered after the polls closed, it may cast doubt on the entire election process regardless of whether the election was actually flawed or not.

I have reviewed the article concerning the Sequoia software that was left unprotected on a publicly available server. I see this as unfortunate but vastly different from the Diebold incident. In the Sequoia case, the software was "leaked" by a government contractor not by Sequoia. Also, the software that was leaked was for systems that display election results, i.e. systems that use raw voter data not systems, such as the voting machine, that gather raw data. This is a tremendous difference because as long as the raw voter data is intact, the true outcome of an election can be determined. In Diebold's case, the software released was for the voting machines that gather the raw data which is inherently more serious. The next significant difference is that the Sequoia code released was binary machine code. This type of software is significantly more difficult to use. The article states that the binary code must be reverse engineered in order to understand how it works. I agree with that assessment. The article also states that this process "is not hard to do". I strongly disagree with that assessment. Although it is certainly possible to reverse engineer binary code, I believe, based on my work with assembly language and binary programming that the reverse engineering process for binary code would be at least hundreds, if not thousands of times more difficult than analyzing software where the source code and programmer comments were available.

There are other points of attack that, depending on the access gained, could seriously disrupt an election. For example, successful attacks on the system that develops the election definition files that are loaded into the voting machines or the back-end server that evaluates the results could create enough confusion to delay election results until the errors are determined and corrected. Typically, though, these areas are much more difficult to access. In an actual election setting, the set of internal controls, physical locks, secured areas and limited access computers, if configured correctly, greatly reduce the risk of these systems being compromised regardless of the strengths or weaknesses of security features in the actual software. I believe this extra security, above and beyond the security of the particular software, greatly reduces the likelihood that someone will be able to access this part of the system, and increases the expertise required of an attacker that chooses this portion of the election system as a target.

As part of my analysis, I asked numerous questions regarding Sequoia's implementation of the voter interface as well as the entire election package. I believe, based on the answers I received and the results in the two reports on the Diebold system that the Sequoia units are more secure. This, however, does not mean that they are perfect. There are several areas where the security of the Sequoia system could be improved over time. Suggestions regarding some proposed improvements could be compiled and forwarded to your office upon request

While I believe Sequoia's approach to be inherently better than Diebold's, the damage done to Diebold by having its source code placed on the Internet cannot be overstated. Secrecy does not, by itself, ensure security. However, the probability of success of most attacks increases as information regarding the target increases. Bank robbers, for example, study their targets before robbing them. Computer hackers electronically survey their targets by "footprinting" them before attacking. I would expect people who attack voting systems to follow the same pattern. Therefore, since Diebold's source code has been made available I would expect people to be studying this software and developing hardware/software items to take advantage of the Diebold voting machines in some future election.

On the other hand, the Sequoia voting machine software is still secret. As people have not had the opportunity to evaluate the Sequoia software, they have a significantly lower likelihood of mounting a successful attack on a Sequoia voting machine. However, based on what I have learned about Diebold's and Sequoia's voting systems, perhaps an evaluation by a trusted independent entity, such as SAIC that was employed by Maryland, and a set of technical standards listing minimum security performance criteria, would add security and peace of mind concerning the voting process to all.

I hope this provides the information you requested concerning the Diebold and Sequoia voting systems. Please contact my supervisor, Board Member Scott Scherer, or myself at your convenience if you have any questions or require any additional information.